EXHIBIT D

DECLARATION OF DONALD VILFER

I, Donald Vilfer, declare as follows:

1. I am one of the owners at Vilfer & Associates, Inc., dba Digital Evidence Ventures, a computer forensics and litigation support company headquartered in Roseville, California. I am a non-practicing attorney and former Supervisory Special Agent with the Federal Bureau of Investigations, last in charge of the White-Collar Crime and Computer Crimes unit, including the Computer Forensics team. I have over 30 years of experience as an investigator and expert and have provided expert testimony in over 100 cases before Federal and state courts, administrative bodies and the International Trade Commission. I regularly provide Continuing Legal Education training to attorneys in the area of digital forensics and am a Lecturer for the Digital Forensics class at the University of California Davis Master's in forensic science program. Attached is a true and correct copy of my CV. I have personal knowledge of the facts stated in this Declaration and, if called as a witness, could and would testify competently to those facts.

2. In March of 2021, I was retained by the Federal Defenders of New York, Inc. to provide digital forensics services and expert consultation, including evaluating evidence provided in discovery related to WhatsApp messages purportedly sent by defendant along with text messages with other people. I was provided with six pdf files that represented information obtained from the cell phone of Stephanie Clifford. Much of the pdf content consisted of what I was told were photos taken by a government agent of the screen on the phone of Stephanie Clifford. One pdf was a series of photos of a phone screen displaying what appears to be conversations with phone number 917-603-[redacted] who was listed as "Luke." Another pdf was also a series of photos taken of a phone, showing messages being purportedly sent to number 917-613-[redacted]. There were no replies from this number in the photos provided. The next pdf was a photo of a phone showing the "About" information for that device, a Galaxy S8 with number 818-355-[redacted]. Another pdf shows a series of photos of a phone screen with text conversation with number 917-293-[redacted] referenced as "Elizabeth (Publisher)." The next pdf is a series of photos of a phone, first showing a photo of Michael Avenatti followed by text conversation with a contact of the same name. The final pdf received was an email from Clark Brewster to Matthew Podolsky and Robert Sobelman of the United States Attorney's Office referencing a pdf attachment he calls "the accumulation of text communications between M. Avenatti and Stephanie Clifford covering the time period of his legal representation."

3. Typically in an investigation involving digital evidence, the digital data is acquired using industry-accepted and proven digital forensic tools that preserve the data in an identical format that can later be verified as being the same as the original data stored on the device. In the case of mobile devices, Cellebrite is the most commonly used tool used to acquire the evidence in a forensically sound manner that will allow for later authentication. Cellebrite and similar tools allow for the examiner to not only acquire the files, such as the databases text messages are stored in, but also to recover and document the metadata about the files such as the date created and modified. The tool will also calculate the hash value, often called a digital fingerprint, of the evidence so it can be verified as being the same as what was on the original device, allowing for authentication. In that the tools are forensic tools, they are comprehensive, often recovering deleted messages and all other available communications and information about activity on the device.

4. The pdf files provided by the government fall far short of being acceptable as evidence of digital data. The pdf files depict photos taken of the screen of a phone and offer none of the authenticating information found through the use of forensic tools. With the simple photos of the screen, there is no way to know if the messages are actually associated with the participants or numbers shown. It is very easy to fabricate a series of messages and then change contact information so it appears the messages were with a different person in the contact database. Even if the messages were not fabricated, the selection of what is displayed for a photo of the screen could have been carefully chosen to exclude parts of a conversation or entire conversations. Even prior to the creation of the photos, the user could have deleted select messages to change the context of messages remaining. A forensic extraction of the device could possibly reveal if either of these events occurred.

5. As an example of how unreliable the provided photos are, the photos that begin at Bates USAO374 00007097 first show some highlights of conversations purportedly with the contact Elizabeth. Those highlights include an October 11 message that begins with “It should go up next time too”. However, that message is not captured in the provided photos even though the photos include other messages from October 11.

6. The attachment provided by the attorney for Stephanie Clifford is equally problematic. I regularly instruct attorneys in the Continuing Legal Instruction classes I teach that paper evidence of electronic files is insufficient and generally not accepted by courts. The attachment submitted to the government by Stephanie Clifford’s attorney consists of a simple string

of text that is titled "WhatsApp chat with Michael Avenetti." WhatsApp is a messaging app used across various digital platforms that stores the messages in a database on the device. Even if a consumer application could be used by someone such as Clifford or her attorney to download messages from the app, the result here appears to be a simple text file that is easily edited. There is no preservation of the conversation that can be authenticated as genuine. Additionally, it is unlikely such an application would recover deleted messages that might be recovered by forensic tools. Whatever was used here to create the text file obviously did not recover conversations with third parties wherein Stephanie Clifford may have discussed the circumstances related to defendant.

7. My review of the printout from Stephanie Clifford's attorney also revealed it is clearly incomplete and does not include all of the content of conversations between Mr. Avenati and Clifford.

8. In investigations that involve digital evidence from mobile devices, the standard practice is to use industry-accepted forensic tools to create a preservation of the data for review. Having received the text file from Clifford's attorney, the best practice would have been for the government agents to then request Clifford's phone for a full extraction. This would have ensured the ability to authenticate the messages, possibly resulted in the recovery of deleted messages and revealed all relevant data that may have been on the device, including discussions with third parties about the allegations or circumstances. The forensic preservation would not have been limited to an export from one app but would have preserved SMS message, MMS or multimedia messages and messages using other apps. This is not what happened in this case. Instead, the government has relied on a text file of questionable origin and photos of Clifford's screen on her phone that those photos by themselves illustrate not all of the messages were collected. The government was in possession of her phone at some point for the photos and could have conducted a forensic preservation to ensure authenticity and completeness but for whatever reason chose not to.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct, and that this declaration was executed on May 1, 2021 in Roseville, California.

Donald Vilfer

Donald E. Vilfer, JD, CFE

Professional:

Vilfer & Associates, Inc., dba Digital Evidence Ventures 2002-present. Founding partner for a Firm that emphasizes computer forensics, eDiscovery and fact-finding in support of complex litigation or referral for prosecution. Representative clients include law firms, state and local government, high-tech firms, aircraft manufacturers, financial institutions and school districts. Cases have included investigation of fraud, theft of intellectual property, computer crimes, employee misconduct, sexual harassment, cell phone location and defense of complex fraud. Extensive experience in obtaining and analyzing computer and cell phone forensic evidence. Experience as an expert witness and court-approved expert in multiple state and Federal jurisdictions as well as the International Trade Commission, having provided sworn testimony over 100 times.

University of California, Davis April 2018-present (full quarter class periodically as scheduled). Lecturer in Digital Forensics for the Masters in Forensics Science Program.

Califorensics 2002-2017. Founder and President of Digital Forensics and Investigative Services firm that served clients nationwide. Sold in 2013 and remained on as Director of Digital Forensics and eDiscovery.

Perry-Smith LLP, 2001-2002, Senior Director, Litigation Support and Investigative Services Group. Led the Litigation Support and Investigative Services practice area for Sacramento's largest regional accounting firm. Supported attorneys in civil and criminal litigation.

Federal Bureau of Investigation, 1986-2001.

1996-2001, Supervisory Special Agent for the White-Collar Crime and Computer Crimes Squad. Conducted and oversaw the investigation of white collar crime and computer crimes. Achieved successful prosecutions in the areas of Securities Fraud, Bank Fraud, Embezzlement, Intellectual Property Rights, Computer Crimes and Bankruptcy Fraud. Oversaw the largest Intellectual Property Rights case in the FBI. Supervised the FBI Computer Forensics Team (CART) and the FBI participation on the High-Tech Task Force. Supervised an international investigation of a series of computer intrusions into financial institutions, resulting in the arrest and conviction of those involved.

1994-1996, Supervisory Special Agent for the Rapid Start Team. At FBI Headquarters, Washington D.C., managed a team of professionals responsible for the on-site management of major cases and crisis worldwide on over 50 cases at venues from the White House to the Oklahoma City bombing command post. Led a project to develop an automated litigation support package for complex white-collar cases. Assisted with implementing automated analysis for Innocent Images project.

1986-1994, Special Agent. Investigated violent crimes, fugitive matters and white-collar crime. Five year FBI SWAT team member. While assigned as Special Agent, Washington D.C. field office, was the case agent an investigation of an international multi-billion dollar bank fraud (BCCI). Oversaw a team of agents and financial analysts responsible for gathering relevant evidence and tracing proceeds. Conducted investigation and asset tracking throughout the US, England, the Cayman Islands and Abu Dhabi.

Donald E. Vilfer, JD, CFE
(continued)

As Assistant Division Counsel, provided legal advice and instruction to FBI Agents in criminal, civil, and employment law areas. Reviewed affidavits for search warrants and court orders.

Delaware Ohio County Prosecuting Attorney's Office, 1986. Prosecuted criminal cases and successfully briefed and argued an appeal.

Education: Bachelor of Science, Criminal Justice/Pre-Law, Bowling Green State University, 1982.

Ohio State University College of Law, Juris Doctorate, 1986.
National Moot Court Team member, advancing to the national level.

Specialized Training: Access Certified Examiner (ACE) certification for Computer Forensics and Decryption.

Certified in Physical and Logical Analysis of cell phones and mobile devices along with additional training in cell phone location evidence.

Four months training at the FBI Academy, including courses in White Collar Crime.

50 Hour Certified Fraud Examination course, including investigation, computer crime, law and accounting. Received CFE Certification.

Advanced White-Collar Crime courses during tenure with the FBI.

One week Computer Crimes course for FBI Supervisors.

Advanced Computer Forensics training, including Windows Registry analysis and Mac OS forensics. Incident Response (hacking) training.

Network Forensics and Cell Phone Location training.

FBI Computer Security class.

FBI class for Supervisory Special Agents over Computer Crimes investigations.

Continuing Legal Education Instructor, *Computer Forensics for Attorneys* and other courses

Frequent guest and consultant to media on crime and computer forensics matters.

FBI Instructor for International Law Enforcement Training Academy in Budapest.

Publication: Incorporating Cell Phone Data into Your Investigations
The AWI Journal-September Vol. 9 No. 3 (2018)

Affiliations: Member of the Ohio Bar (inactive status).
Member of the Association of Certified Fraud Examiners.

Expert Testimony: Federal Courts, State Courts, FINRA, California Office of Administrative Hearings, International Trade Commission.